

O problema não é você, é o fabricante

Luiz Eduardo, Security CTO, HPE Networking

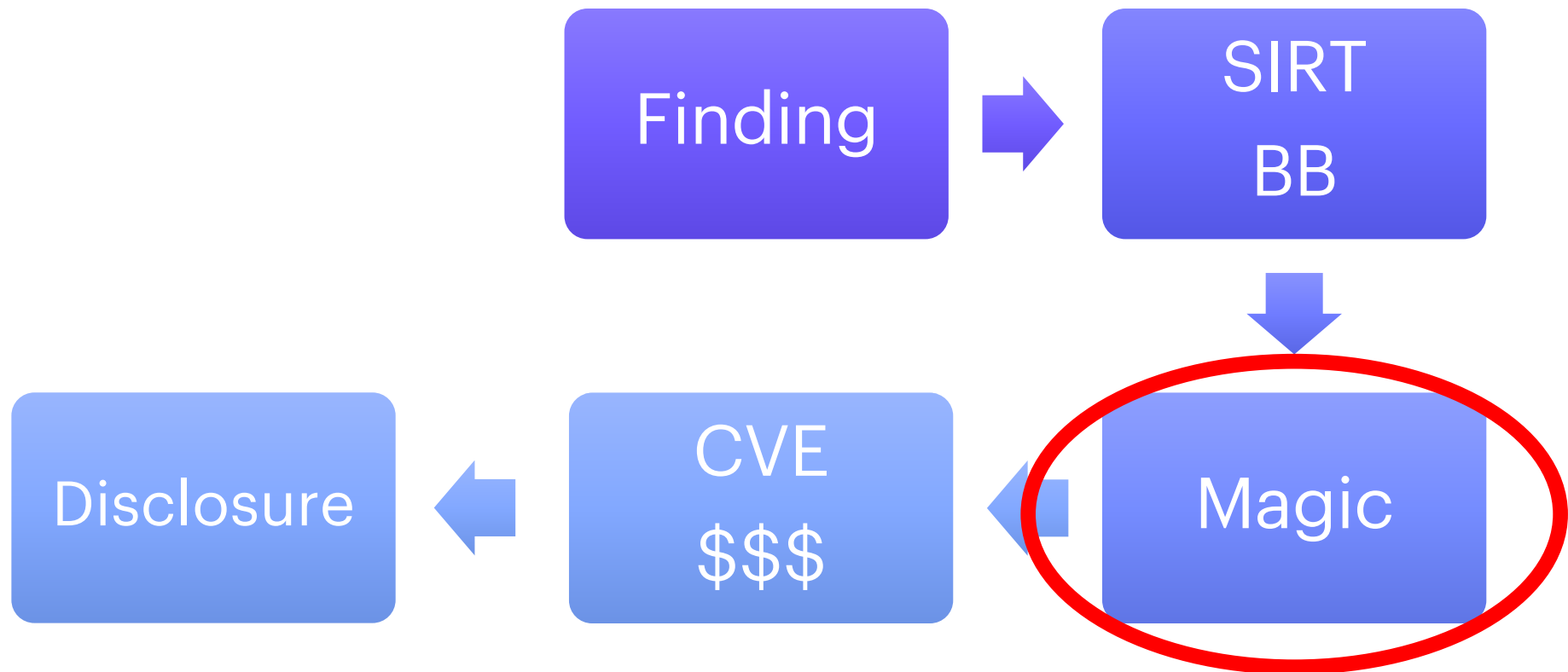




OF COURSE NOT

FRIEND

The usual process







VISITE NOSSA COZINHA

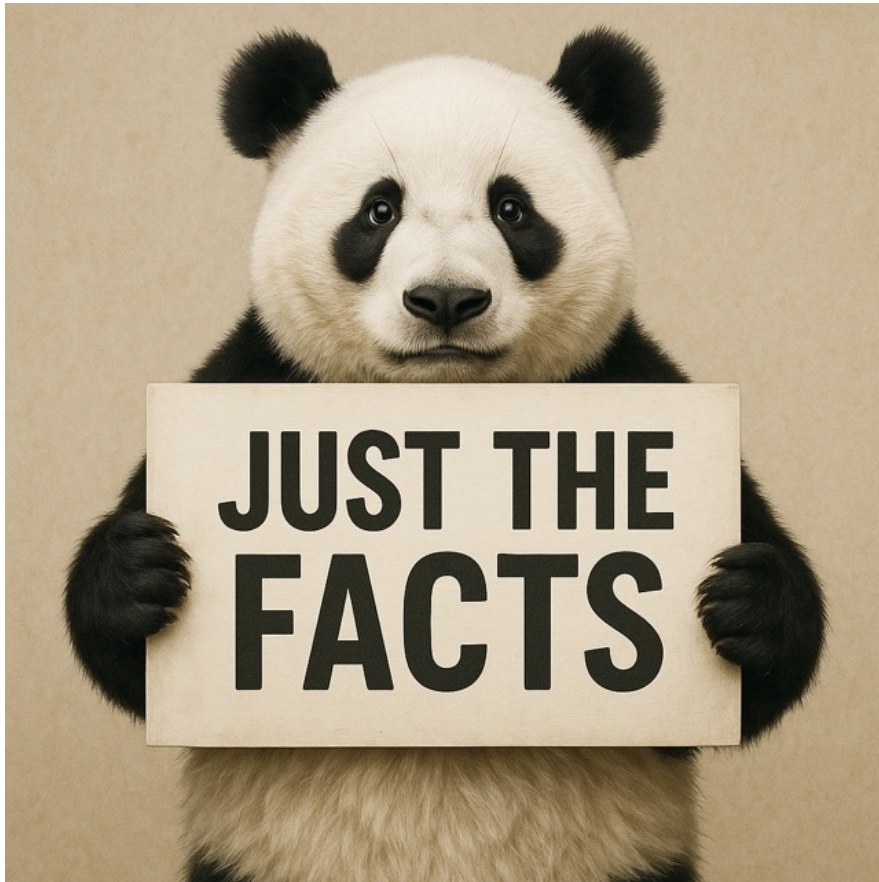
LEI MUNICIPAL Nº 11.617/94

**Confira
nosso padrão
de HIGIENE**

Not that you care about it, but...



Facts



Multiple supported versions, what does that mean?

- Code dependencies
- release schedule/ QA
- Code complexity
- fundamental changes
- systemic bugs



“We are paying ‘researchers’? Who are they?”




- v1ntage
- 4NTIQUE
- u_g0t_pl41d
- susp3nder
- br0cco1337
- Unkn0wn
- 1RON1C
- pwnt13
- st4rbucko
- B34RDYBOY
- Khagendra8

And still, in this day and age

▼ Activity

All Comments Work Log History Activity Timepiece

▼  [REDACTED] added a comment - 26/Feb/19 6:34 AM

As I understand, crash is triggered by user entering >33 characters in login username field. As per documentation, max length of username is 32 characters. Hence, please request customer to not create username larger than 32 characters. Closing ticket as WONTFIX.







MINIMIZE RISK



What to do with this?

The image is a composite of three screenshots illustrating a security vulnerability, likely a Denial of Service (DoS) attack using a malformed HTTP request.

Top Screenshot (Web Browser): Shows a GET request to `/html/json.html?method:uiGetLogEvents&req_mode=4&num_entries=1000`. The response status is `HTTP/1.1 200 OK` from `Server: eHTTP v2.0`. The response body contains a malformed HTML snippet: `<html></html>`. A red box highlights the `Cookie: sessionId=` header in the request.

Bottom Left Screenshot (Terminal): Shows a PuTTY window with the command `login a: <html></html>` entered. The output shows "Pre-authentication banner message from server:". A red box highlights the command input.

Bottom Right Screenshot (Login Form): Shows a login form with a "sessionId:" label and an input field. A red box highlights the input field, which contains the session ID. An "OK" button is visible.

Shodan is (not always) your friend



How to get ignored



Let me guess.... *Not the kind of response you want to hear?*

Not going to lie. You going from smarmy and patronizing to exploit begging me is pretty amusing.

Once again, you come at me with hostility and back off when you realize you're in the wrong or maybe out of your depth.

Do yourself and your organization a favor:

Take a look below. Stop being an dick.



Dear Vendors

- Have an updated /.well-known/security.txt file on your website
- Have a disclosure policy
- Have “a” process
- (Or have something)
- Closing the loop: Security Advisories





Instituição de ensino e pesquisa **sem fins lucrativos** com a missão de oferecer conhecimento para futuros profissionais de **cibersegurança**.

Contamos com programas exclusivos para **pessoas negras** e **mulheres**, bem como conteúdo e **cursos livres**.

Apoie



Chave Pix:
doacao@mentebinaria.com.br

<https://www.mentebinaria.com.br>

Thank You

<https://www.linkedin.com/in/luizeduardo/>

